

Vitals Suite (GMRV*5.0*38)

**Deployment, Installation, Back-Out, and Rollback
Guide**



April 2019

Department of Veterans Affairs (VA)

Office of Information and Technology (OIT)

Revision History

Date	Description	Author
April 2019	Initial Release	REDACTED

Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software and should be structured appropriately to reflect these procedures.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Guide is to be completed prior to Critical Decision Point #2 (CD #2). The expectation is that this document will be updated, as needed, throughout the lifecycle of the project.

Table of Contents

1. Introduction	1
1.1. Purpose.....	1
1.2. Dependencies.....	1
1.3. Constraints	1
2. Roles and Responsibilities.....	2
3. Deployment	4
3.1. Timeline.....	4
3.2. Site Readiness Assessment.....	4
3.2.1. Deployment Topology (Targeted Architecture)	4
3.2.2. Site Information (Locations, Deployment Recipients)	4
3.2.3. Site Preparation	4
3.3. Resources	4
3.3.1. Facility Specifics	4
3.3.2. Hardware	4
3.3.3. Software.....	5
3.3.4. Communications	5
3.3.4.1. Deployment/Installation/Back-Out Checklist.....	5
4. Installation.....	6
4.1. Pre-installation and System Requirements	6
4.2. Platform Installation and Preparation.....	6
4.3. Download and Extract Files	6
4.4. Database Creation.....	6
4.5. Installation Scripts	6
4.6. Cron Scripts.....	7
4.7. Access Requirements and Skills Needed for the Installation	7
4.8. Installation Procedure	7
4.8.1. GMRV*5.0*38 Vista Installation	7
4.8.2. Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 Installation.....	8
4.8.2.1. Vitals and Vitals Manager GUI Methods of Installation.....	8
4.8.2.2. Vitals Lite DLL Methods of Installation	10
4.9. Installation Verification Procedure	12
4.10. System Configuration	12
4.11. Database Tuning	12
5. Back-Out Procedure	12
5.1. Back-Out Strategy.....	12
5.2. Back-Out Considerations	12
5.2.1. Load Testing	12

5.2.2. User Acceptance Testing	12
5.3. Back-Out Criteria.....	13
5.4. Back-Out Risks.....	13
5.5. Authority for Back-Out.....	13
5.6. Back-Out Procedure	13
5.7. Back-out Verification Procedure.....	14
6. Rollback Procedure	14
6.1. Rollback Considerations	14
6.2. Rollback Criteria.....	14
6.3. Rollback Risks.....	14
6.4. Authority for Rollback	14
6.5. Rollback Procedure	14
6.6. Rollback Verification Procedure	14

List of Tables

Table 1: Roles and Responsibilities	2
Table 2: OI Field Offices	6
Table 3: Files to be Downloaded	6
Table 4: HPS Clinical Sustainment Contacts.....	13

List of Figures

Figure 1: Shortcut Icons for Vitals and Vitals Manager	9
Figure 2: Test Vitals38 Properties	10

1. Introduction

The Vitals Suite (GMRV*5.0*38) consists of Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3. This document describes how to deploy and install Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort. In cases where a non-developed commercial off the shelf (COTS) product is being installed, the vendor provided User and Installation Guide may be used, but the Back-Out Recovery strategy still needs to be included in this document.

1.1.Purpose

The purpose of this plan is to provide a single common document that describes how, when, where, and to whom the Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 will be deployed and installed as well as how they are to be backed out and rolled back. The plan also identifies the resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

1.2.Dependencies

The Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 projects are for installation on a fully patched VistA system. There are two Graphical User Interface (GUI) components and a Dynamic-Link Library (DLL) that should be running on a Windows system.

1.3.Constraints

Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 and the associated Mumps patches are expected to be installed on existing VistA platforms. The hardware may reside at local or regional data centers. Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 utilize existing nationally released security controls to control access.

2. Roles and Responsibilities

No one single entity oversees decision making for deployment, installation, back out and rollback of Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3. The Release Agent and Application Coordinators under the Veterans in Process will approve deployment and install from a product development perspective. If an issue with the software arises, then the Area Managers and other site leadership will meet, along with input from Patient Safety and Health Product Support, to initiate a back out and rollback decision of the software in accordance with the Information Technology (IT) Operations and Services personnel. The following table provides Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 project information.

Table 1: Roles and Responsibilities

Team	Phase / Role	Tasks
IT Operations and Services personnel	Deployment	Plan and schedule deployment (including orchestration with vendors)
IT Operations and Services personnel	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.
Site personnel.	Deployment	Test for operational readiness
IT Operations and Services personnel The IT support will need to include person(s) to install the Kernel Installation and Distribution System (KIDS) build as well as the personnel to deploy the GUI – which may be done on each machine, a shared network and/or the Citrix access gateway	Deployment	Execute deployment
IT Operations and Services personnel. The IT support will need to include person(s) to install the KIDS build as well as the personnel to deploy the GUI – which may be done on each machine, a shared network and/or the Citrix access gateway	Installation	Plan and schedule installation
N/A – will work under the VistA authority to operate (ATO) and security protocols.	Installation	Ensure authority to operate and that certificate authority security documentation is in place
N/A – no equipment is being added.	Installation	Validate through facility point of contact (POC) to ensure that IT equipment has been accepted using asset inventory processes

Team	Phase / Role	Tasks
N/A – no new functionality is being introduced.	Installations	Coordinate training
Facility chief information officer (CIO), IT Operations, and Services personnel	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)
Hardware and System support – no changes. Software support will be the Health Product Support (HPS) Clinical Sustainment team.	Post Deployment	Hardware, Software and System Support

3. Deployment

The deployment is planned as a standard VistA National Patch Module patch rollout. Once approval has been given to nationally release, the GMRV*5.0*38 patch will be released from the National Patch Module. At this point, it will be available for installation and deployment at all sites.

Scheduling of test/mirror installs, testing and deployment to production will be at the site's discretion. It is anticipated there will be a 30-day compliance period.

3.1. Timeline

There is no specific timeline for deployment. This is considered a maintenance release and installation will be at the site's discretion, within the constraints of the compliance period for the release.

3.2. Site Readiness Assessment

This section discusses the locations that will receive the Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 deployment.

3.2.1. Deployment Topology (Targeted Architecture)

Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 will be deployed to each VistA instance. That will include local sites as well as regional data processing centers. The executables will also be deployed to the Citrix Access Gateway.

3.2.2. Site Information (Locations, Deployment Recipients)

The initial deployment will be to IOC sites for verification of functionality. Once that testing is completed and approval is given for national release, Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 (GMRV*5.0*38) will be deployed to all VistA systems.

The Production (IOC) testing sites are:

- Tuscaloosa VA Medical Center
- VA Salt Lake City Health Care System

3.2.3. Site Preparation

There is no special preparation required for Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3. A fully patched VistA system is the only requirement.

3.3. Resources

N/A

3.3.1. Facility Specifics

N/A

3.3.2. Hardware

N/A

3.3.3. Software

N/A

3.3.4. Communications

Service Delivery and Engineering (SDE) Field Implementation Services will be sending out an action item and National Change Order prior to the release of Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 advising them of the upcoming release.

Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 will be deployed using the standard method of patch release from the National Patch Module rather than a phased deployment. When patch GMRV*5.0*38 is released, the National Patch Module will send a notification to all the personnel who have subscribed to those notifications.

3.3.4.1. Deployment/Installation/Back-Out Checklist

The deployment and installation will be performed by site support personnel once it is nationally released.

4. Installation

4.1.Pre-installation and System Requirements

Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 assume a fully-patched Vista system.

4.2.Platform Installation and Preparation

[VistA] This patch should be loaded during non-peak hours to minimize disruption to users. Installation will take less than 5 minutes. Users may remain on the system.

[GUI] The time to deploy the GUI will depend on which method the site utilizes for running the executables (network share, Citrix, individual workstation installs, etc.).

4.3.Download and Extract Files

Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 is being released as a PackMan message distributed through the National Patch Module combined with a .ZIP file containing the GUI file(s).

REDACTED

This transmits the files from the first available server. Sites may also elect to retrieve files directly from a specific server.

Sites may retrieve the software and/or documentation directly using Secure File Transfer Protocol (SFTP) from the REDACTED directory at the following OI Field Offices:

Table 2: OI Field Offices

Location	Site
REDACTED	REDACTED
REDACTED	REDACTED

Documentation can also be found on the VA Software Documentation Library at:

<https://www.va.gov/vdl/>

Table 3: Files to be Downloaded

File Name	File Contents	Download Format
GMRV_5_0_P38.ZIP	GUI Files (Vitals and Vitals Manager executables; Vitals Lite DLL)	Binary
GMRV_5_0_P38_SRC.ZIP	GUI Source Files	Binary

4.4.Database Creation

N/A

4.5.Installation Scripts

N/A

4.6.Cron Scripts

N/A

4.7.Access Requirements and Skills Needed for the Installation

Installation of Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 requires the following to install:

- Programmer access to the VistA instance and the ability to install the KIDS build.
- Citrix Access Gateway (CAG) installs – access/ability to upload to the CAG.
- Network Share installs – access/ability to upload executables to the network share location.
- Individual workstation installs – access/ability to push executables to required workstations.

4.8.Installation Procedure

4.8.1.GMRV*5.0*38 VistA Installation

1. Choose the PackMan message containing this patch and invoke the **INSTALL/CHECK MESSAGE PackMan** option.
2. Select Kernel Installation & Distribution System Option: Installation
 - 1 Load a Distribution
 - 2 Verify Checksums in Transport Global
 - 3 Print Transport Global
 - 4 Compare Transport Global to Current System
 - 5 Backup a Transport Global
 - 6 Install Package(s)
Restart Install of Package(s)
Unload a Distribution
3. From this menu, must use the **[Backup a Transport Global]** option to create a back out message.
4. From this menu, the following options may be used:
 - Compare Transport Global to Current System
 - Verify Checksums in Transport Global
5. Use the Install Package(s) options and select the package GMRV*5.0*38
6. When prompted **Want KIDS to INHIBIT LOGONs during the install? NO//**, respond NO.
7. When prompted **Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO//**, respond NO.

4.8.2.Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 Installation

The ZIP file contains the Vitals and Vitals Manager GUI executables and Vitals Lite DLL. Download the ZIP file and extract all the files.

4.8.2.1. Vitals and Vitals Manager GUI Methods of Installation

The following methods of installation of Vitals and Vitals Manager are available. Sites' choice of which method(s) to use will depend upon IT Operations and Services personnel/Veterans Integrated Service Network (VISN) policies, Local Area Network (LAN) performance or other local circumstances. User requirements, physical location and methods of connection to the VA network may warrant more than one of the options below to be used.

Note: Vitals Manager is not needed for every user. This is designed for users who are responsible for the management of the Vitals package for this server.

Network (shared) installation:

This method is typically the simplest to maintain, providing the local network infrastructure is robust enough to handle the additional traffic caused by users running the GUI executables (Vitals.exe and VitalsManager.exe) across the LAN.

The GUI executables (Vitals.exe & VitalsManager.exe) and help files (VITALS.chm & VITALSMANAGER.chm) are copied to a network shared location. Users are provided with a desktop shortcut to run Vitals.exe & VitalsManager.exe directly from the network shared drive. The necessary command line parameters (Vista server address or name and RPC Broker Port number) are entered in the Target field of the shortcut properties.

At the time of a Vitals and/or Vitals Manager version update, the copy of Vitals.exe & VitalsManager.exe and the help files are replaced, on the network share, with the new version.

Any users requiring access to another site's Vitals.exe and/or VitalsManager.exe system can be given an alternate desktop shortcut with command line parameters appropriate to the intended target Vista system.

If a user requires access to an older or newer version of Vitals.exe or VitalsManager.exe (e.g. for testing purposes), then a different version of Vitals.exe and/or VitalsManager.exe can be placed in a separate network location, and the user can be supplied with an appropriate alternate shortcut (different Target path and different Vista server command line parameters).

Citrix installation:

The GUI executables (Vitals.exe & VitalsManager.exe) and help folder and files (VITALS.chm & VITALSMANAGER.chm) are installed and run from a remote workstation, and the user views the remote workstation's screen on their local workstation.

For the local site users, this method is on a similar level to the **Network (shared) installation** above. The users' workstations require only an appropriate shortcut (and the necessary CAG infrastructure).

Note: For issues with CAG, please contact the local or national help desk.

Local workstation installation:

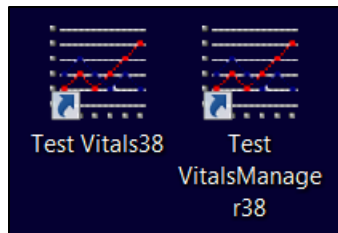
This is the “standard” method of installation where the GUI executables (Vitals.exe & VitalsManager.exe) and help folder and files (VITALS.chm & VITALSMANAGER.chm) are installed on and run from the user's local workstation. This method of installation initially requires the distribution and installation of a Microsoft Software Installation (MSI) file to each user's workstation, typically accomplished via SCCM. This is outside the scope of the Sustainment team. A National package (Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3) has been prepared and made available to Regional COR Client Technologies leadership.

Manual install:

This method is used for users who wish to have a production instance and a non-production instance running on the same machine. An example would be users who are testing this software or need to have access to a pre-production (mirror) VistA instance.

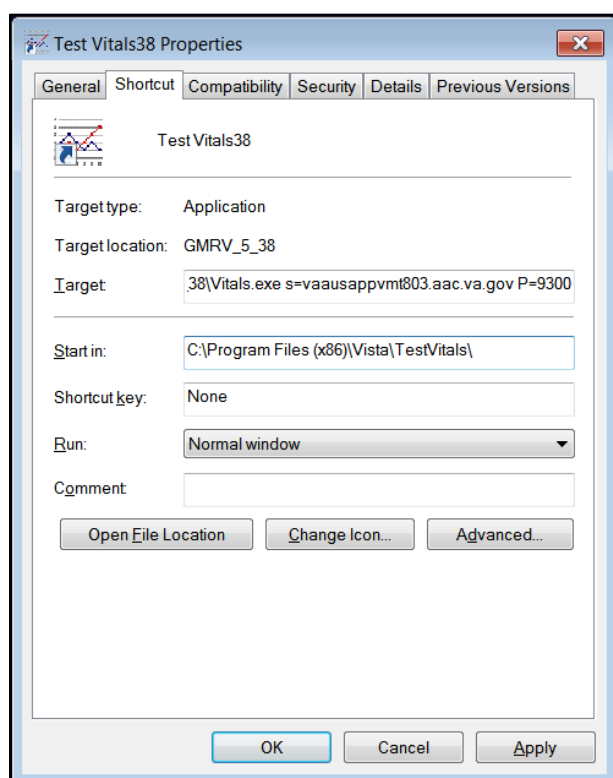
1. Locate the GMRV_5_0_P38.ZIP and unzip the file.
Copy the contents of the zip archive (the 2 GUIs and the 2 help files) to a test directory, for example, C:\VitalsTest. A new directory may need to be created.
Note: Administrator rights are required for the PC used to complete this step.
2. Create Shortcut(s) and name it/them **Test Vitals38** and/or **Test VitalsManager38**. This is to give the user another visual cue that these are not the normal Vitals icon.

Figure 1: Shortcut Icons for Vitals and Vitals Manager



3. Determine the domain name server (DNS) server name or internet protocol (IP) address for the appropriate VistA server.
4. Determine the Broker Remote Procedure Call (RPC) port for the VistA account.
5. Enter the IP (or DNS name) and RPC port in the Target field of the Shortcut properties (or use ServerList.exe).

Figure 2: Test Vitals38 Properties



Note: The server and port number shown above are for example only.

4.8.2.2. Vitals Lite DLL Methods of Installation

The following methods of installation of Vitals Lite are available. Sites' choice of which method(s) to use will depend upon Regional/VISN policies, Local Area Network (LAN) performance or other local circumstances. User requirements, physical location and methods of connection to the VA network may warrant more than one of the options below to be used.

Network (shared) installation:

This method is typically the simplest to maintain, providing the local network infrastructure is robust enough to handle the additional traffic caused by users running the DLL (GMV_VitalsViewEnter.dll) across the network.

The DLL (GMV_VitalsViewEnter.dll) and help file (GMV_VitalsViewEnter.chm) are copied to the network shared location that contains the Computerized Patient Record System (CPRS) executable. Users will access the DLL via CPRS's coversheet.

At the time of a Vitals Lite version update the copy of GMV_VitalsViewEnter.dll and the help file are replaced, on the network share, with the new version. Specifically, the CHM file should replace the existing HLP file.

If a user requires access to an older or newer version of GMV_VitalsViewEnter.dll (e.g. for testing purposes), then a different version of GMV_VitalsViewEnter.dll can be placed in a separate network location and the user be supplied with an appropriate alternate shortcut (different Target path and different Vista server command line parameters).

Citrix installation:

The DLL (GMV_VitalsViewEnter.dll) and help file (GMV_VitalsViewEnter.chm) are installed and run from a remote workstation, and the user views the remote workstation's screen on their local workstation.

For the local site users, this method is similar to the Network (shared) installation above. The users' workstations require only an appropriate shortcut (and the necessary CAG infrastructure).

Note: For issues with CAG, please contact the local or national help desk.

Note: In GMRV*5*38, the DLL cannot find its help file when both files are in any folder other than the folder with CPRS (CPRSChart.exe). If users require the help file while using Vitals Lite, it will need to be installed in the same folder as CPRS. This is a known bug and pre-dates GMRV*5*38. It will be fixed in a future patch.

Local workstation installation:

This is the “standard” method of installation where the Vitals Lite (GMV_ViewEnter.dll) and help file (GMV_VitalsViewEnter.chm) are installed on and run from the user's local workstation.

Note: There is a national SCCM package to help sites or ITOPS distribute the Vitals Lite DLL. However, in GMRV*5*38, the DLL cannot find its help file when both files are in any folder other than the folder with CPRS (CPRSChart.exe). If users require the help file while using Vitals Lite, it will need to be installed in the same folder as CPRS. This is a known bug and pre-dates GMRV*5*38. It will be fixed in a future patch.

Manual install:

Unzip the GMRV_5_0_P38.ZIP file and move the files to an appropriate directory and/or workstation.

Windows 7 & 10:

- For 64-bit machines: **C:\Program Files (x86)\Vista\Common Files**
- For 32-bit machines: **C:\Program Files\Vista\Common Files**

Note: The above directories are the standard approach. However, in GMRV*5*38, the DLL cannot find its help file when the DLL and help file are in any folder than the folder with CPRS (CPRSChart.exe). If users require the help file while using Vitals Lite, it will need to be installed in the same folder as CPRS. This is a known bug and pre-dates GMRV*5*38. It will be fixed in a future patch.

1. Rename the current version of the DLL (5.0.37.2) to GMV_VitalsViewEnter.dll.bkup.37.
2. Copy the new version of the DLL (5.0.38.3) into the same folder.
3. Rename the GMV_VitalsViewEnter.hlp to GMV_VitalsViewEnter.hlp.bkup.37.
4. Copy the GMV_VitalsViewEnter.chm into the same folder.

To switch between versions, reverse the steps above - rename the current release DLL (5.0.37.2) to GMV_VitalsViewEnter.dll, rename the new version of the DLL (5.0.38.3) to GMV_VitalsViewEnter.dll.bkup.38, rename the current release HLP file to GMV_VitalsViewEnter.hlp, and rename the CHM file to GMV_VitalsViewEnter.chm.bkup.38.

4.9. Installation Verification Procedure

[VISTA] Verify the checksum of routine GMV38PST is equal to the checksum listed on the patch description.

[GUI] Launch both the Vitals and Vitals Manager GUIs and verify the splash screen now announces that version 5.0.38.3 is running. Log into the desired server and verify that a version mismatch is not received. Launch the Vitals Lite DLL from within CPRS and verify the About screen now announces that version 5.0.38.3 is running.

4.10. System Configuration

N/A

4.11. Database Tuning

N/A

5. Back-Out Procedure

5.1. Back-Out Strategy

[Vista] To revert the Vitals and/or Vitals Manager version, re-install patch GMRV*5.0*36. To revert the Vitals Lite version, re-install patch GMRV*5.0*37.

[GUI] To revert the Vitals and/or Vitals Manager GUI(s), the prior GUI(s) would have to be redistributed. For Vitals this is v5.0.36.2 and for Vitals Manager this is v5.0.36.1. To revert the Vitals Lite DLL, the prior DLL (v5.0.37.2) would have to be redistributed.

The HPS Sustainment Clinical team is available to assist with sites that have misplaced their backup PackMan message. They will also give you the instructions on downloading the executables.

5.2. Back-Out Considerations

5.2.1. Load Testing

No load testing was performed on Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3. This was a maintenance release to correct defects discovered in Vitals Lite v5.0.37.2, Vitals v5.0.36.2, and Vitals Manager v5.0.36.1. There was no additional functionality included.

5.2.2. User Acceptance Testing

User acceptance testing was conducted by the two test sites listed in section 3.2.2.

The sites followed the provided test plan and executed the test cases according to the plan for the third build of GMRV*5.0*38. The sites either passed or failed any item based on testing. The tests were performed by users at each site who are familiar with using the application. The test cases were then delivered to the HPS Clinical Sustainment team. Any items that failed were re-

developed and then sent back to the sites for the next build and further acceptance testing following the same process. Once in production, the same final test cases from the last build were tested in production. No subsequent builds were created as the test cases passed and sites signed off on concurrence for release of the product.

5.3.Back-Out Criteria

Back-out would only be considered if there was a catastrophic failure that causes loss of function for the applications and/or a significant patient safety issue.

5.4.Back-Out Risks

Backing out Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 would result in the re-instatement of the issues that were addressed.

In addition, there is a risk that the process, which would be performed only in an emergency situation, would significantly impact patient care due to the interruption.

5.5.Authority for Back-Out

The Area Manager has the final authority to require the rollback and accept the associated risks.

5.6.Back-Out Procedure

These steps assume that the only reason to consider a back-out for Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3 is in the event of a catastrophic failure.

1. Contact the HPS Clinical Sustainment implementation team to notify them there has been a catastrophic failure with Vitals Lite v5.0.38.3, Vitals v5.0.38.3, and Vitals Manager v5.0.38.3. Use the following contacts:

Table 4: HPS Clinical Sustainment Contacts

Name & Title	Email	Telephone Number
REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED

2. If the decision is made to proceed with back-out and rollback, the HPS Sustainment Clinical team will be available to assist sites that have misplaced their backup PackMan message and provide the instructions on downloading the executables.
3. [VistA]
 - a. Open the Backup MailMan Message
 - b. At the **Enter message action (in IN basket): Ignore**// prompt Enter **X** for [**Xtract PackMan**]
 - c. At the **Select PackMan function:** prompt select [**INSTALL/CHECK MESSAGE**].
The old routine is now restored.
4. [GUI] Coordinate with the appropriate IT support, local and regional, to schedule the time to install GMRV*5.0*36 for Vitals and Vitals Manager and GMRV*5.0*37 for Vitals Lite, and to push out / install the previous GUI executables and DLL.

5. Once GMRV*5.0*36 for Vitals and Vitals Manager and GMRV*5.0*37 for Vitals Lite have been installed, verify operations before making available to all staff.

5.7.Back-out Verification Procedure

1. Ensure the v5.0.36.1 and v5.0.36.2 executables and the v5.0.37.2 DLL launch properly.
2. Perform site-specific testing appropriate to the areas where the catastrophic failure was identified.

6. Rollback Procedure

6.1.Rollback Considerations

N/A

6.2.Rollback Criteria

N/A

6.3.Rollback Risks

N/A

6.4.Authority for Rollback

The Facility CIO has the final authority to require the rollback and accept the associated risks.

6.5.Rollback Procedure

Back-out will automatically rollback version.

6.6.Rollback Verification Procedure

N/A